I numeri (pseudo)primi di Fermat

Francesco Cavalli, Bollettino dei docenti di matematica, dicembre 1996

Pierre de Fermat (1601-1665), spesso definito il re dei dilettanti, è stato uno dei massimi matematici del XVII secolo. Si interessò anche di analisi, geometria, geometria analitica e calcolo delle probabilità, ma viene ricordato principalmente per i suoi contributi alla teoria dei numeri. Passò tutta la vita lavorativa quale avvocato a Tolosa, occupandosi di matematica nel tempo libero. Non viaggiò mai, ma fu in corrispondenza con altri matematici del suo tempo, tra cui Mersenne e Pascal.
Tra i suoi enunciati in teoria dei numeri, il più famoso è certamente il cosiddetto "ultimo teorema di Fermat" secondo cui l'equazione $\mathbf{x^n + y^n = z^n}$ non ammette soluzioni intere per $n > 2$. Fermat affermava di averne trovato una dimostrazione, ma soltanto nel 1993 Wiles ne ha saputo dare una dimostrazione completa.
Ma molti altri enunciati sulla teoria dei numeri (numeri primi, somme di potenze, equazioni diofantee) sono dovuti a Fermat che si è riferito spesso all'Aritmetica di Diofanto (III sec.), una delle prime opere conosciute che si occupa di questo tema.

I numeri primi di Fermat sono numeri primi della forma $F_n = 2^{2^n} + 1$
Fermat ipotizzò che tutti i numeri F_n fossero primi, anche se non pretese di averlo dimostrato. Circa un secolo più tardi, Eulero (1707-1783) scoprì che F_5 non è un numero primo.

$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$

$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$

$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$

$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$

$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$

sono numeri primi, mentre il successivo

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$ è divisibile per 641.

Si sa oggi che i numeri F_n fino a $n = 21$ sono tutti composti, anche se non di tutti si è ottenuta una fattorizzazione completa.

A tutt'oggi non si sa se esistano altri valori di n con F_n numero primo, anche se ciò sembra poco probabile.

Per iniziare lo studio dei numeri di Fermat, ci si può dapprima chiedere quali numeri della forma 2^n sono primi

Teorema

$2^n + 1$ è primo solo se n è una potenza di 2

Dimostrazione

Se n è dispari, allora $2^n + 1$ è divisibile per 3

Infatti $n = 2m + 1 \quad \Rightarrow \quad 2^{2m+1} + 1 = 2 \cdot 4^m + 1$

$4 \equiv 1 \pmod 3 \quad \Rightarrow \quad 2 \cdot 4^m + 1 \equiv 2 + 1 \equiv 0 \pmod 3$

Se n ha un sottomultiplo dispari, cioè $n = d\,2^k$

$2^n + 1 = 2^{d2^k} + 1 = a^d + 1$ che è divisibile per $a + 1$.

$a \equiv -1 \pmod{a+1} \quad \Rightarrow \quad a^d \equiv (-1)^d \equiv -1 \pmod{a+1}$

$a^d + 1 \equiv 0 \pmod{a+1}$

È ora necessario, prima di proseguire la teoria relativa a questi numeri, affrontare un altro importante teorema di Fermat.

Il piccolo teorema di Fermat

Teorema

Se p è un numero primo, allora per ogni a ($1 \le a < p$), p divide $a^p - a$

Dimostrazione

Questa dimostrazione, dovuta a Eulero, è per induzione. Altre dimostrazioni, più recenti, si rifanno al calcolo con le congruenze e alla teoria dei gruppi.

per $a = 1$, ovviamente, $a^p - a = 0$ è divisibile per p

Ipotesi d'induzione: $a^p - a$ è divisibile per p

$$(a+1)^p - (a+1) = a^p + \binom{p}{1} a^{p-1} + \ldots\ldots + \binom{p}{p-1} a + 1 - (a+1)$$
$$= a^p - a + \binom{p}{1} a^{p-1} + \ldots\ldots + \binom{p}{p-1} a$$

Tutti i coefficienti $\binom{p}{k} = \frac{1}{k!}\, p\,(p-1) \ldots\ldots\ldots (p-k+1)$ sono divisibili per p, essendo $k < p$, e p numero primo; $a^p - a$ è pure divisibile per p (ipotesi di induzione) e dunque anche $(a+1)^p - (a+1)$ è divisibile per p.

Ad esempio, essendo 43 primo, si ha che $2^{43} - 2$, $3^{43} - 3$, ... $42^{43} - 42$ sono tutti divisibili per 43.

L'inverso del piccolo teorema di Fermat, invece, non è vero, anche se in passato qualcuno (ad esempio i Cinesi), ne ha fatto un criterio per stabilire se un numero è primo.

Il più piccolo numero che non verifica l'inverso del piccolo teorema di Fermat è 341.

Infatti $2^{341} - 2$ è divisibile per 341, ma $341 = 11 \cdot 31$

$2^{341} - 2 = 2\,(2^{340} - 1) = 2\,(2^{10 \cdot 34} - 1)$

$2^{10 \cdot 34} - 1$ è divisibile per $2^{10} - 1 = 1023 = 3 \cdot 341$ (vedi (3) del teorema successivo)

I numeri non primi che verificano il piccolo teorema di Fermat sono detti pseudo-primi.

341 è pseudo-primo solo in base 2; infatti $3^{341} - 3$ non è divisibile per 341.
Ma esistono anche numeri assolutamente pseudo-primi, cioè tali che $a^n - a$ è sempre divisibile per n per ogni valore di a. Il più piccolo è $561 = 3 \cdot 11 \cdot 17$
Si può dimostrare che esistono infiniti numeri pseudo-primi.

Riprendendo i numeri F_n si può ora dimostrare che, se non sono primi, sono almeno pseudo-primi.

Teorema
$F_n = 2^{2^n} + 1$ verifica il piccolo teorema di Fermat,
cioè $F_n \mid (2^{F_n} - 2)$ ($2^{F_n} - 2$ è divisibile per F_n)

(il simbolo $a \mid b$ indica che a è divisore di b)

Dimostrazione

La dimostrazione è rielaborata dal testo [3]

(1) si dimostra facilmente per induzione che $k + 1 \leq 2^k \quad (k > 0)$

(2) $k + 1 \leq 2^k \Rightarrow 2^{k+1} \mid 2^{2^k}$

(3) $a \mid b \Rightarrow 2^a - 1 \mid 2^b - 1$

infatti, $b = m\,a \Rightarrow 2^b - 1 = 2^{m\,a} - 1 = (2^a - 1)(2^{a(m-1)} + \ldots\ldots + 1)$

(4) dalla (3), applicando la (2) si ottiene: $2^{k+1} \mid 2^{2^k} \Rightarrow 2^{2^{k+1}} - 1 \mid 2^{2^{2^k}} - 1$

(5) $(2^{2^n} + 1)(2^{2^n} - 1) = 2^{2.2^n} - 1 = 2^{2^{n+1}} - 1$

(6) $F_n = 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1 \mid 2^{2^{2^n}} - 1 \mid 2.\,2^{2^{2^n}} - 2 = 2^{2^{2^n}+1} - 2 = 2^{F_n} - 2$

Quindi se F_n non è primo, è sicuramente almeno pseudo-primo. Si può anche supporre che Fermat, conoscesse questo teorema ma, ignorando l'esistenza di numeri pseudo-primi, avesse concluso che tutti i numeri F_n fossero primi.

Molte altre proprietà interessanti sono collegate ai numeri di Fermat. In particolare una che riguarda la costruzione dei poligoni regolari.
Gauss (1777-1855) dimostrò nel 1801 che il numero di lati di un poligono regolare costruibile con riga e compasso deve avere la forma:

$N = 2^k \; q_1 \, q_2 \, ... \, q_r \, ,$ (dove q_i sono numeri primi di Fermat).

Lo stesso Gauss propose un metodo per costruire il poligono regolare di 17 lati.
Sono quindi costruibili i poligoni con 3, 5, 15, 17, 51, 85, 257, 65537, ... lati, mentre non lo sono quelli con 7, 9, 11, 13, 19, 21, ... lati.
Non so se qualcuno si sia davvero cimentato a costruire il poligono regolare di 65537 lati!

Bibliografia

[1] E.T.Bell "I grandi matematici" (Sansoni 1966)

[2] André Weil "Teoria dei numeri" (Einaudi 1993)

[3] Waclaw. Sierpinski "250 problèmes de théorie élémentaire des nombres" (Jacques Gabay 1992).

[4] Pirre de Fermat "Osservazioni su Diofanto (Boringhieri 1969)

[5] Federico Enriques "Questioni riguardanti le matematiche elementari" (Zanichelli 1987)